**IT Applications**

**Unit 4, Outcome 2**

**Ch 8, Security Measures, Security Procedures, p 243**

**Security Procedures**

**Organisations require policies to define how an information system should be used.**

**Communication**

1. The conventions for good email usage are:

* The subject heading should be used, and be meaningful.
* The message priority should be set correctly.
* Each email should contain a signature of the person sending an email.
* A privacy disclaimer should be at the end of each email sent.

1. Electronic data interchange (EDI) is an application-to application communication of data between organisations. Its main role is to process purchase orders. It links the supplier, manufacture and purchaser via their networks to automatically process transactions.

**Storage**

1. **File-naming conventions**
   1. The 3 pieces of information that each document should contain in its filename is:

* **Datestamp:** A date that indicates the timeliness of a document. This information is different from the meta-data saved with each file that indicates when the document was created and when it was last saved.
* **Variation:** Identifying which version of the file is saved. This allows employees to keep track of which version they worked on.
* **Name:** Something meaningful that can identify the document.

1. **Location of files**
   1. In a network an organisation may set a directory structure to control where employees store their files.
2. **Backups**
   1. Distinguish between
      1. **Full backup-** Copies all the files from a device to a storage medium. It can take considerable time and is usually preformed once over a period of time (such as week, fortnight or month).
      2. **Differential backup-** Only copies those files those files that have been changed since the last full backup. Restoration of data would involve restoring files from the full backup and the differential backup.
      3. **Incremental backup-** It is similar to differential backup except it users more than two backup media.
   2. A **backup log** includes the workstation or system backed up, the software used for backup, the number, type and storage location of the backup media. It also includes the date of individual backups and list of files and folders to be backed up.

* 1. A restoration log should include:
* The workstation or system restored to.
* The date of restoration.
* A list of files or folders restored.
* The backup media used (including date and volume name and number).
* The reason for restoration.
  1. The use of volume name or number is useful because it describes where the backup data has to come from. In an organisation where there are multiple servers, the volume name might be used to indicate which server the backup tape belongs to.

**Backup timeline, p 247**

1. The grandparent-parent-child system is the suggested backup. The parent is the second oldest copy of the file. The child is the most recent copy of the file.
2. Hard disks are used as a first-level backup medium because they can restore data quickly.

**Location of backup files**

1. The various options in locating backup files are that they can be stored in a location that is safe from theft, and damage caused by extremes of temperature or disasters.

**Archiving/destruction**

1. The distinction between archiving and destruction is that destruction involves deletion only whereas archiving is the process of copying files to long-term storage, then deleting them from the hard disks.
2. The archived files are stored on the same type of media as backups.

**Disaster Recovery Strategies**

1. A disaster recovery plan is a document that tells an organisation what steps are needed to restore the company operations, including computing, in the event of a disaster.

A disaster recovery plan has four key elements.

1. **Emergency Plan**

* Explains the specific steps to be taken in the event of a natural disaster.
* The emergency plan should contain the information about names and contact details of people trying to notify, including the management and emergency services. It should also include evacuation procedures for all involved including the removal of backup tapes or equipment. It will also include return procedures.

1. **Backup Plan**

* Covers the procedures that the company has to follow for using file backups to restore computer systems. This may occur in the event of equipment failure, sabotage, theft of equipment and vandalism.
* This will include the location of alternative sites and equipment in case the normal computer facility has been destroyed.
* The location of backup data, suppliers and equipment.

1. **Recovery Plan**

* A recovery plan includes specific procedures for restoring the full information processing capacity of the organisation.
* It will cover both hardware and software replacement.

1. **Test Plan.**

* The test plan will contain information about simulating a variety of disasters and different recovery needs.

**Evaluating the effectiveness of data security measures, p 250**

1. **Integrity of data**

**Data integrity depends on its accuracy, reliability and timeliness.**

* 1. The integrity element depends on its accuracy, reliability and timeliness. It can be evaluated against storage, communication and disposal because in the table that shows how it is to be measured. You may expect that 90% of the time, information arrives at its destination whereas you always expect that data can be saved correctly.

1. **Security**
   1. Security can be evaluated, both physically and software by ensuring that hackers cannot get into the system, this indicates that your security measures are working. Physical protection can be evaluated to see if theft or damage to the equipment has decreased since the procedures were implemented.
2. **Ease of retrieval**
   1. Things that assist ease of retrieval are observance of file and folder naming conventions that everyone in the company knows. Using correct file extensions is important because it allows recognition by application software.
   2. Backed up files should be restored so if crashes occur then the backups are needed, to determine whether they can be restored in the time frame.
3. **Currency of files**
   1. The most recent file is easily identifiable if sequential file-naming conventions are used.

**Evaluating the effectiveness of data security management strategies**

1. The ways in which an evaluation of the effectiveness of data security management strategies can occur are:

* Who can get access to the physical environment and access to the network?
* What anti-virus software are you using and how often is it updated?
* How often are the passwords changed and checked?
* How vulnerable is the system to outsiders?
* Do you have a business continuity plan in the event of a disaster?